TVA Standard Programs and Processes	**TITLE** **Mobile and Remote Access to TVA's Information Resources**	**TVA-SPP-12.3** **Rev. 0000** **Page 1 of 8** Effective Date 04-01-2006

Responsible Peer Team: IT Business Strategy Council

Approved by:	Robert J. Beecken Vice President, Nuclear Support	07-19-2005 Date
Approved by:	Diane J. Bunch, Chair Senior Vice President, Information Services	07-14-2005 Date
Approved by:	Amy T. Burns Vice President, Bulk Power Trading	05-25-2005 Date
Approved by:	Joseph R. Bynum Executive Vice Executive Vice President, Fossil Power Group	06-08-2005 Date
Approved by:	Janet C. Herrin Senior Vice President, River Operations	06-09-2005 Date
Approved by:	James D. Keiffer Senior Vice President, Marketing	05-25-2005 Date
Approved by:	Paul R. LaPointe Senior Vice President, Procurement	05-26-2005 Date
Approved by:	John E. Long, Jr Executive Vice President, Administrative Services	06-15-2005 Date
Approved by:	Randy Trusley Vice President & Controller	05-21-2005 Date
Approved by:	Van Wardlaw Vice President, Transmission and Reliability	07-07-2005 Date

Current Revision Description

Initial issue.

Table of Contents

1.0 PURPOSE

The purpose of this TVA Standard Programs and Processes (TVA-SPP) is to define TVA's Mobile and Remote Access Program and provide instruction for implementing TVA's Policy on Mobile and Remote Access to TVA Information Resources.

2.0 SCOPE

This TVA-SPP applies to TVA employees, contractors, grantees, and employees of other federal agencies, state and local governments, business partners, and other organizations and individuals who access TVA's network and/or information systems from mobile and remote systems or devices. Access methods include but are not limited to dial-up, broadband or wireless.

3.0 PROCESS

3.1 Roles and Responsibilities

Senior Vice President of Information Services (SVP, IS)

The SVP, IS, is responsible for establishing, managing and enforcing TVA's Policy on Mobile and Remote Access to TVA Information Resources and associated implementing procedures, programs and standards, both within TVA and with respect to external business relationships with external business partners and other federal agencies and ensuring compliance with the policy.

Office of Inspector General (OIG)

The OIG is responsible for promoting the efficiency, effectiveness, and integrity of TVA's information resources including mobile and remote systems and devices. This responsibility is accomplished, in part, by performing independent and objective security audits, investigations, and inspections to evaluate compliance of the program to established federal laws, regulations, and accepted best practices.

TVA Officer

Each Officer is administratively and operationally responsible for overseeing the implementation and enforcement of TVA's Mobile and Remote Access Program within their respective business unit.

Designated Approving Authority (DAA)

The DAA formally approves the operation of a General Support System (GSS), a Major Application (MA) and approved network access points at an acceptable level of risk.

Manager and Equivalents

Each TVA Manager (all levels) or other equivalent is responsible for the enforcement of compliance with TVA's Mobile and Remote Access Program within their business unit.

3.1 Roles and Responsibilities (continued)

TVA Employee, Contractors, and Others

All TVA employees, contractors, grantees, other federal agencies, state and local governments, business partners, and others who have mobile and remote access to TVA's information systems are responsible for complying with this TVA-SPP.

3.2 Mobile and Remote Access Program Instruction

The SVP, IS:

A. Manages TVA's Mobile and Remote Access Program.

B. Serves as TVA's principal point of contact for all matters relating to mobile and remote access to TVA's information resources.

C. Authorizes and approves network access points.

D. Coordinates with the applicable DAA on authorizing mobile and remote access to TVA's information resources.

E. Develops, establishes, and promulgates policies, procedures, and standards for mobile and remote access consistent with TVA's Information Technology (IT) Security Policy.

F. Reviews, revises, and cancels policies, procedures, practices and standards as necessary to ensure compliance with federal laws and regulations and accepted best practices.

G. Oversees and enforces policy and guidance pertaining to the program elements.

3.3 Mobile and Remote Access Program

A. The key elements of TVA's Mobile and Remote Access Program have two levels of access:

1. **Web Access** - Users without need for administrative or elevated access to TVA systems or applications. Access will be limited to select Web-based information and applications. Access may be from TVA- or non-TVA-owned systems and devices. Additionally, TVA may specify security configuration requirements dependant on the information accessed or processed. These requirements will be specified, agreed to, and implemented prior to access being granted.

2. **Restricted Access** - Users with need for administrative or elevated access to TVA systems or applications. Access will be network-level (i.e., the mobile or remote system or device will appear as if it is part of TVA's corporate network). Access will be restricted to TVA-owned systems and devices, except for TVA business partners, contractors or other external stakeholders who meet TVA-specified security requirements as defined by TVA's IT Security Policy. These requirements will be specified, agreed to, and implemented prior to access being granted.

3.3 Mobile and Remote Access Program (continued)

B. TVA-owned mobile and remote systems must conform to TVA-specified configuration requirements including security control requirements specified by the applicable GSS and/or MA system security plan.

C. Technical support will be provided to TVA-owned systems and devices only.

D. Users of all mobile and remote systems will protect the confidentiality, integrity, and availability of TVA's information and information systems commensurate with the level of risk and magnitude of harm resulting from the loss, misuse, unauthorized access, or modification of the information or information system.

E. The use of wireless technology to connect to TVA's network infrastructure will be restricted to approved network access points.

3.4 Process for Gaining Mobile or Remote Access to TVA's Information

To request mobile or remote access to TVA's Information Systems, complete and submit Form TVA 17349, ID Request Form for Distributed Computer Systems to the IT Service Center (ITSC) according to the instructions provided with the form.

4.0 RECORDS

4.1 QA Records

None

4.2 Non-QA Records

Form TVA 17349, ID Request Form for Distributed Computer Systems

5.0 DEFINITIONS

Availability - The security goal that generates the requirement for protection against intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data and unauthorized use of system resources.

Confidentiality - The security goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and in transit.

General Support System (GSS) - An interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people, as well as provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Individual applications may be from the same or different organizations.

5.0 DEFINITIONS (continued)

Information - An instance of a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization, or in some instances, by a specific law, Executive Order, directive, policy, or regulation.

Information System - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Integrity - The security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has when it has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).

Major Application (MA) - An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to, or comprise many individual application programs and hardware, software, and telecommunication components. MA can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

Mobile - Any computing device that is capable of being operated while being physically transported from one location to another when used in conjunction with computing and networking technology.

Network - Communication capability that allows one user or system to connect to another user or system and can be part of a system or a separate system. Examples of networks include local area network (LAN) or wide area networks, including public networks such as the Internet.

Network Access Point - A hardware device that acts as a communication hub for users of a wireless device to connect to a wired LAN.

Portable - Anything that is capable of being carried or moved about.

Remote - A geographical location wherein sufficient distance exists as to prohibit, in any way, physical corporate network connectivity via contiguous cable or wire when used in conjunction with computing and networking technology.

Risk - The possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.

Wireless - A medium of transfer wherein information (voice or data) is transferred between communicating devices by use of radio signals.

Wireless Computer - A process which combines the use of mobile computing with wireless networking to provide dynamic mobile access to corporate information resources.

6.0 REFERENCES

A. The TVA requirements include:

1. Information Technology Security Policy.

2. IS-SPP-10.10 - Guidelines for Purchase, Installation and Support of Handheld Computers (HHC) or Personal Digital Assistants (PDA).

3. IS-SPP-10.24 - Wireless Local Area Network Access.

4. IS-TI-TC-001 - Wireless Access Point Installation.

B. The statutory requirements include:

1. Federal Information Security Management Act

2. Freedom of Information Act of 1980 Public Law (P.L.) 93-502

3. Government Paperwork Elimination Act, P.L. 105-277

4. Privacy Act of 1974, P.L. 93-579

5. Paperwork Reduction Act of 1995, P.L. 104-13

6. Records Management by Federal Agencies, 44 United States Code, Chapter 31, January 6, 1997

C. Federal agency guidance provides additional requirements for the management of federal information resources and critical infrastructures. These documents include:

1. Office of Management and Budget Circular A-130, Appendix III

2. Homeland Security Presidential Directive-7

3. Executive Order 13231, Critical Infrastructure Protection, October 14, 2001

4. Standards, Guides and Guidelines issued by the National Institute of Standards and Technology